公租房背景下 NB-IoT 安全智能锁系统解决方案 *

沙 涛 [1a]，刘梦君 [1a, 1b†]，李 丹 [2, 3]，刘树波 [3]

(1. 湖北大学 a. 计算机与信息工程学院, b. 教育学院, 武汉 430062; 2. 湖北省水利水电科学研究院, 武汉 430070; 3. 武汉大学 计算机学院, 武汉 430072)

摘 要：针对公租房市场中租赁客户身份复杂、变动频繁，难以安全有效管理、阻止租户转租难题，设计了一个基于 NB-IoT（Narrow Band Internet of Things）的安全智能锁系统。它利用位置证明和时间戳加密机制，实现了对房屋安全门锁权限统一管理，并可防止远程开锁、重放攻击及中间人攻击。理论分析和测试结果表明，所提方案能够在安全高效管理公租房屋、阻止用户的转租的同时，具备较低的计算和通信开销。

关键词：公租房；安全门锁；NB-IoT；位置证明

中图分类号：TP309.2 doi: 10.3969/j.issn.1001-3695.2018.03.0132

NB-IoT security smart lock system solution under background of public rental housing

Sha Tao[1a], Liu Mengjun[1a, 1b†], Li Dan[2, 3], Liu Shubo[3]

(1. *a. School of Computer & Information Engineering*, *b. School of Education Hubei University*, *Wuhan* 430062, *China*; 2. *Hubei Research Institute of Water Conservancy & Hydroelectric Power*, *Wuhan* 430070, *China*; 3. *School of Computer*, *Wuhan University*, *Wuhan* 430072, *China*)

Abstract: Due to the complex and fast changing tenant constitution, it is of great challenge to manage public rental housing for government. This paper proposed a secure smart lock system based on the NB-IoT technology (Narrow Band Internet of Things) , which aiming at solving the secure and long-term concentrate management and subletting problem encountered by managers. It could efficiently manage the houses, prevent users from opening lock remotely, as well as resist the Replay-Attack and Man-in-the-Middle Attack via the location proof and timestamp-based encryption schemes. Intensive theoretical analysis and test results show that the proposed scheme can solve all these problems with low computation and communication overhead.

Key words: Public rental housing; Safety door lock; NB-IoT; Location proof

0 引言

随着房屋租赁市场形态的不断演变，房屋租赁客户与房屋租赁方的成分构成发生了较大的变化。其特点表现在房屋租赁客户构成复杂多变，房屋出租方出现诸多新生主体，房屋租赁活动由过去单纯的市场行为转变为市场与政策行为并存。在这种情况下，公租房的出现带来了的新的管理与安全挑战[1~3]。

公租房出现的初衷是给予相关弱势群体政策照顾，保障公民的合理住房权益，维护社会公平。这些出发点决定了公租房的社会公益性，也决定了公租房难有商业出租房同等的收益。目前公租房由政府倡导，企业承办，通过对于市场上现有的公租房项目进行调研分析发现，其实施中遇到了租金收缴困难、运营管理缺乏标准、租户不合理使用、社区安全性不足等问题。随着各个区县政府的积极推进，公租房入住家庭日益增加，后期管理所面临的问题日益增大。用户拖欠租金现象影响项目可持续运营，租户对物业管理不理解、推脱物业费，租户生活条件发生变化后不符合租住条件，且将公租房转租他人等问题严重影响公租房市场。同时由于其租赁性质，人员身份构成复杂，若不加以力度管理，也会对社区安全带来许多负面影响。公租房的特点在于其人流变化频繁，对于房屋的出租与收储需要大量人员去管理，在有限的收益条件下，如何在安全高效高水准地做好公祖房管理工作、解决上述问题的前提下，减少公租房管理成本，成为了摆在公租房管理方面前的一道难题。因此设计一种无人值守安全门锁是提高公租房安全高效管理水准的关键途径[4-5]。

窄带物联网 NB-IoT[6, 7]（Narrow Band Internet of Things）

收稿日期：2018-03-21；**修回日期：**2018-04-28 **基金项目：**国家自然科学基金面上项目（41671443）；湖北省自然科学基金项目（201711111201003）；湖北省教育厅自然科学基金项目（201711131001003）；武汉市科技局应用基础研究计划资助项目（2016010101010024）

作者简介：沙涛（1996-），男，江苏泰兴人，本科生，主要研究方向为物联网、信息安全；刘梦君（1988-），男（通信作者），湖北黄冈人，博士，讲师，主要研究方向为移动/无线网络、移动社交/分布式系统上的安全与隐私（lmj_whu@163.com）；李丹（1981-），男，博士研究生，主要研究方向为数据挖掘、信息安全；刘树波（1970-），男（蒙古族），教授，博士，博导，主要研究方向为物联网安全与隐私保护、数据隐私挖掘与发布．

的出现为解决公租房市场下无人值守门锁系统带来了技术可能。NB-IoT 拥有低速率、低功耗、广覆盖等优点，同时可在原有 2G、3G、4G 网络基站上实现部署升级，具有传统物联网技术所没有的超低功耗特性。而一般意义下的传统门锁系统，如 PIN 码、射频门卡、指纹锁、GPRS 锁等类型[8~1]的门锁，在面对公租房这一应用场景时，功能显得不够充分。PIN 码和射频门卡不能做到用户信息可追踪，在面临公租房这一人员变化频繁的环境，对于钥匙的管理将耗费巨大人力成本和设备成本，同时对于用户信息不能做到联网查询，存在钥匙或门卡丢失及冒用的安全隐患；而射频门卡大都采取明文形式的无线通信，易被劫持开锁指令后伪造门卡，带来安全隐患；同时它们都不支持远程监控门锁设备及管理权限。而支持远程监控的门锁设备，如指纹锁、GPRS 锁，无法做到低功耗并长时间值守于无市电供电的环境下。

不同于一般意义上的门锁系统，公租房场景下将会面对租客转租现象，同时公租房人流密集，在如何提供方便的公租房管理办法同时，保证系统不会被攻破是研究人员必须解决的问题。采用 NB-IoT 技术的安全智能锁系统实现了现有方案所不能实现的痕迹化管理，能够统一管理用户开锁权限且具有超低功耗。但是在使用 NB-IoT 安全智能锁系统的时候，会遇到恶意用户发起的重放[12]、合谋[13]等多种攻击的问题，同时为了解决公租房中存在的转租问题，系统还必须能够识别用户位置信息，防止远程开锁[14]。

针对目前市面上智能锁的功耗过高、公租房实施过程中遇到的转租难题以及采用 NB-IoT 技术遇到的安全问题，本文提出一个解决方案，可大大减少公租房管理成本，同时解决租客构成复杂难以管理、对门锁系统安全性担忧以及不诚实用户远程开锁等问题。

1 系统模型与问题定义

1.1 系统模型

系统主体包括 4 方，分别是智能锁远程管理服务器、安全智能锁终端、用户开锁设备和用户。其中：智能锁远程管理服务器由公租房管理机构管理使用，其职能包括租户资质及账户信息管理，用户秘钥管理，房屋使用信息管理，智能锁位置、状态、密钥信息管理。服务器具备互联网接入功能。安全智能锁终端执行用户身份认证、接收用户开锁指令并记录用户开锁信息。安全智能锁终端采用 2 个超低功耗通信接口，分别为 NB-IoT 模组和 Bluetooth 模组，NB-IoT 模组用于同服务器进行通信，而 Bluetooth 模组用于同用户设备通信。用户开锁设备承载用户智能锁使用 APP，与服务器进行用户与服务器的会话秘钥协商生成、更新，执行用户与安全锁的位置证明、功能数据安全通信。用户开锁设备具有 3G/4G 网络通信接口，Bluetooth 通信接口，指纹识别接口。用户是开锁的发起方，持有设备并安装智能锁使用 APP 或微信小程序，每次开锁时要对其所在位置生成位置证明。所以保障智能锁系统安全工作关键点在于保证用户所在位置的位置证明可信及确保开锁设备及安全智能锁之间通信链路安全。

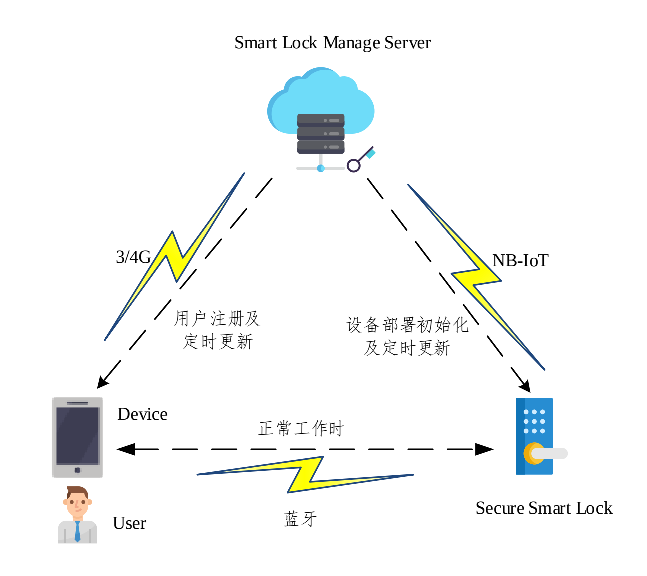


图 1 安全智能锁方案框架

1.2 安全模型

系统中，智能锁远程管理服务器是可信的，也即它会管理用户和智能安全锁终端密钥及保护密钥安全，对于拥有开锁权限的用户分发对应锁的密钥，对于撤销权限的用户会注销当前密钥。而用户是半诚实的，即守信用户会按照约定方案来使用安全智能锁系统，且用户不会主动泄露密钥，但是用户会尽可能利用系统所给与的信息进行开锁操作，不排除恶意攻击者主动攻击行为，如重放攻击、合谋攻击。安全智能锁是安全可控的，不考虑被暴力破坏。

由于对密钥的管理采用无线通信，系统处于开放环境中，因此环境周围充满不可信因素。潜在安全威胁包括：窃听攻击—获取开锁指令中用户信息；重放攻击—截获用户开锁指令，后续发送给智能锁；合谋攻击—在用户设备与智能锁之间改变发送者身份；先拒绝服务攻击，再重放攻击等。此外，用户身份过期需要请求智能锁远程管理服务器重新分配密钥，APP 与服务器之间采用安全传输层协议（TLS）。更换智能安全锁终端需要短信或邮箱确认。所有对安全智能锁系统的攻击设定在用户进行开锁操作之间，包括上述所有潜在安全威胁。

1.3 问题描述

对于系统中四个实体智能锁远程管理服务器(Smart Lock Manage Server, SLMS)、安全智能锁终端(Secure Smart Lock, SSL)、用户开锁设备(Device, D)和用户(User, U)。因为公租房管理涉及到租客房屋使用权限管理，传统实物钥匙开锁存在回收钥匙不便，用户钥匙存在冒用及遗失等诸多不便，对于每一个门锁还需记录其开锁信息，同时，如果使用无线网络进行管理时，需要对各种恶意攻击进行防御，常见如假冒攻击、重放攻击、合谋攻击等。

具体地，某一时刻用户 U_i 通过安全智能锁 SSL_i 发送开锁指令(instruction, I)，为了防止假冒、重放及合谋攻击，需要周

期地生成用户位置证明(Location Proof, LP)。假定开锁设备 D 足够密集，用户 U_i 发起指令使得 SSL_i 与 D_i 之间完成开锁动作的通信开销为 $Comm_{D_i \to SSL_i}$，本文的问题归结为需要在 U_i 进行开锁操作之前，为其生成不可窜改的真实 LP 证明其与 SSL_i 距离关系，抵御重放、合谋等恶意攻击，并使得 $Comm_{D_i \to SSL_i}$ 最小。

该本方案设计总体目标如下：

（1)拥有开锁设备及用户身份双重认证机制以提高系统可信度；

（2）保证用户开锁密钥唯一性，用户开锁密钥在线生成、更新、撤销管理，能够记录并存档开锁用户信息，使能查询锁状态，起到预警及追踪的功能。

（3）系统拥有前向安全性，能够较好地抵御假冒攻击、重放攻击、合谋攻击等；

此外，设备开锁处理流程因全部在后台处理完成，考虑到智能门锁工作环境，此系统应能在低电压状态下工作，具有低工作能耗的特性以延长设备工作时间。

2　NB-IoT 安全智能锁解决方案

2.1　主要思想

公租房安全运营面临两方面技术难题，一是如何建立用户、智能锁远程管理服务器、安全智能锁终端三方的安全开锁管理机制，防止用户进行远程开锁，二是解决在此过程中的恶意人员伪造或重放攻击开锁。前一问题通过强制用户使用近距离蓝牙通信媒介传输开锁指令来杜绝诚实用户的远程开锁，而为了杜绝恶意用户的合谋远程开锁，本文设计了基于位置证明（Location Proof, LP）的身份验证机制，用户在登录 APP 或微信小程序时，系统将随机地启动用户位置验证，当用户确实处于安全距离范围内，才能正常开锁，从而解决了远距离开锁带来的转租问题。另外，由于系统间采用无线通信，信息容易被截取，本文设计一种时间戳加密机制，任意双方通信时的信息将使用高级加密标准[15]（Advanced Encryption Standard，AES）进行加密以保证安全性，同时添加时间戳信息，防止重放攻击。

围绕着以上 2 个核心技术问题，本文设计了一整套安全开锁及用户高效管理解决方案。具体如下：

2.2　详细方案

本文构建的 NB-IoT 安全智能锁方案中涉及 3G/4G 和 NB-IoT 两种远程通信方式和一种短距离通信方式：蓝牙（Bluetooth）。用户通过 3G/4G 网络登录手机上安装的 APP 软件，获取私密密钥 $k_{U_i}^-$，用于连接安全智能锁发送开锁指令 *Open*() 以及生成位置证明 LP，NB-IoT 用于服务器向安全智能锁下发密钥 $k_{SSL_i}^-$，$k_{SSL_i}^- = k_{U_i}^-$。当用户需要开锁时，首先使用开锁设备 D 登录 APP，此时系统指定部分附近设备为签名设备，用户将自己密钥拆分成多份子密钥 K_i，通过蓝牙发送给各个签名设备。签名设备将使用此子密钥为开锁用户生成一个当前位置证明 LP，开锁设备将这些 LP 打包一起发送给智能锁远程管理服务器，SLMS 对此 LP 进行验证。由于用户即使不诚实也不会将自己私钥共享出去，此过程能够有效避免用户欺骗系统，检测出转租用户。当验证成功时，开锁设备通过蓝牙连接安全智能锁并将包含此位置证明的开锁指令与当前时间信息经过密钥加密后发送给安全智能锁 SSL，SSL 使用 SLMS 通过 NB-IoT 网络下发的密钥对发来信息解密，当解密成功时，表明确认了用户身份和位置信息，锁即开启。此方案规避实物密钥型门锁钥匙遗失产生的风险，同时相比其他通过无线网络的开锁设备易被攻击窃取权限，或被进行远程开锁，本方案提出的基于位置证明的身份验证机制和时间戳加密机制有效地解决了这一问题。非授权方没有密钥无法开锁，同时不在安全智能锁附近的用户无法开锁，当恶意用户试图攻击系统时，上述两种安全机制能有效抵御攻击。NB-IoT 安全智能锁方案的工作流程如图 2 所示。

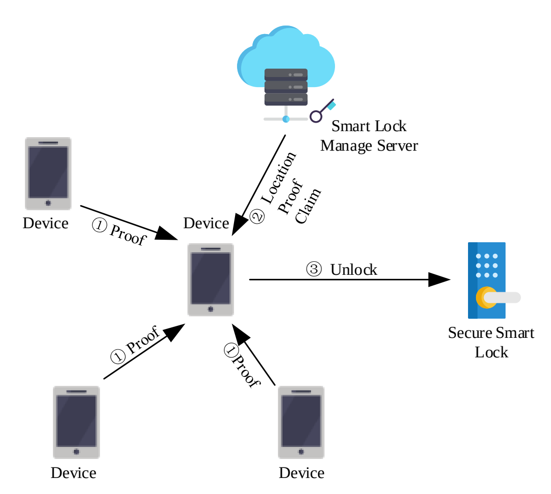


图 2　安全智能锁方案的工作流程图

安全智能锁系统面临最大的问题即安全性问题，本文围绕着如何实现上述设计方案的同时，设计了基于位置证明的身份验证机制和时间戳加密机制，有效的抵御了无线网络通信中几种非常棘手的攻击，其中第一种机制(基于位置证明的身份验证机制, Location Proof-Based Security mechanism, LPBS)通过利用即使是不诚实的用户也不会将自己密钥分享出去的特点，保证了用户生成的位置证明一定是真实的，任何通过假冒或中间者进行远程开锁的恶意用户将会被识别。在第一种机制基础上，本文设计第二种机制(时间戳加密机制, Timestamp Encryption mechanism, TE)，通过精心设计一种开锁指令，令利用重放攻击的恶意用户无法窃取权限进行开锁操作。本文在本章之后部分将对上述两种机制予以展开叙述。

2.3　基于位置证明的身份验证机制

2.3.1 工作原理

位置证明是通过附近多个可信签名设备为请求位置证明的设备，在某一合法距离某一时刻提供的授权的数字签名，请求设备收集此多个数字签名再将其交予管理者验证。在现有共同工作假设中，对于用户 U_i 即使它不诚实的，也不会把自己的私钥 $k_{U_i}^-$ 共享出去，利用这一用户的行为特点，通过 P2P 方式阻止用户之间合谋生成虚假位置证明。具体地，对于每个用户 U_i 所

持有的带有 GPS 功能的移动设备 D_i，设其附近同样具备 GPS 功能为 D_i 生成位置证明的可信签名设备 D_W 有 n 个， D_i 为将要发送开锁指令的设备，除此之外与 D_W 相同， D_W 通过蓝牙为 D_i 生成位置证明，当 U_i 进行开锁操作之前，本文设置 U_i 必须将自己的私钥 $k_{U_i}^-$ 通过 (k,n) 门限秘密共享[16]的方式，将自己的 $k_{U_i}^-$ 分成 n 分子密钥，然后使用安全传输层协议将子密钥分别发送给 n 个 D_W，D_W 将通过将接收到的子密钥嵌入为 D_i 生成的位置证明，并加上自己的数字签名授权。D_i 将所有的生成位置证明汇集经过加密后发送给智能锁远程管理服务器 SLMS，SLMS 会对这些位置证明验证时间地点，验证成功后解密将子密钥恢复出来，SLMS 利用门限秘密共享的特点从这些子密钥中进行恢复操作，如果能够恢复出原密钥，即代表此位置证明是真实的，反之则代表此 U_i 为一个欺骗用户。

通过上述方法，U_i 所在位置必须在允许范围内，否则无法生成合法的位置证明，否则它会因为位置证明验证的时候不合法被拒绝进行开锁操作，或者由于 SLMS 不能通过子密钥恢复出原密钥而被认定没有同附近所有的 D_W 完成证明工作而被拒绝访问。

其中包含的原理为：

（1）对于非授权用户 U，其没有授权私钥 $k_{U_i}^-$，即使生成了合法 LP，也会由于 SLMS 恢复不出授权 $k_{U_i}^-$ 而被识别出来。

（2）对于授权用户 U，若其不在安全位置，却被恶意者劫持了开锁指令，由于 U 不在安全距离范围了，其生成的 LP 将会告知 SLMS 位置证明不合法，进而 SLMS 识别出此为恶意者正在进行开锁操作并拒绝其任何操作。

（3）若用户 U 串谋社区内用户合作欺骗签名设备 D_W，那么对于不在 U 旁边的 D_W，U 无法直接将子密钥发送给 D_W，因为诚实的 D_W 没有侧信道，也即 D_W 无法为其生成位置证明，而如果通过某个在合法位置的用户进行中继，那么 U 必需将其私钥泄露给中继用户。

基于位置证明的身份验证机制中包含三个主要阶段，第一阶段为位置证明生成阶段，第二阶段为位置证明验证阶段，第三阶段为时间戳加密阶段。

2.3.2 位置证明 LP 生成

本方案中涉及到的符号如表 1 所示，

位置证明 LP 生成过程，具体如下：

（1）开锁设备 D：假定开锁设备 D_i 想在某一时间 t 想要进行开锁操作，本文设定 D_i 必须先向周围签名设备 D_W 广播请求生成位置证明，并等待附近签发设备 D_W 的回应后才能进行下一步操作，位置证明生成请求记为 LPR，组成如下：

$$LPR = Comm(ID_{Di}, r_{Di})|t|L \tag{1}$$

其中，ID_{Di} 是 D_i 的唯一身份标志，r_{Di} 是一个随机数，$Comm()$ 是一个 Commitment 机制[17]， Commitment 机制是一种密码学技术，其通过对哈希算法对 ID_{Di} 和 r_{Di} 生成对应的哈希值 $h(ID_{Di}, r_{Di})$，$h()$ 是一个单向不可逆的安全算法，如 SHA256，由于其不可逆性质，任何用户无法在收到 $h(ID_{Di}, r_{Di})$ 后，再算出 ID_{Di} 和 r_{Di} 的值，而智能锁远程管理服务器 SLMS 可以通过后发来的 ID_{Di} 和 r_{Di} 验证此信息有效性，这样既保证了用户身份的无法被改变，同时也能防止用户身份信息泄露给其他参与者。

表 1　重要符号说明

符号	说明
$k_{U_i}^-$	开锁用户的私密密钥
K_i	通过门限秘密共享生成的子密钥
K^+	智能锁远程管理服务器公开密钥
$k_{D_{W_i}}^-$	签名设备私密密钥
$k_{SSL_i}^-$	安全智能锁私密密钥
k_p	临时通信密钥
$E_{k_p}(a)$	使用密钥 k_p 对 a 进行对称加密
$a \mid b$	将信息 a 和信息 b 连接起来
D_i	某一个开锁设备
D_{Wi}	某一对开锁设备位置证明进行签名的设备
SSL_i	某一安全智能锁
ID_{Di}	开锁设备的唯一身份标志
$r_{D_{Wi}}^{i}$	Commitment 机制中 D_{Wi} 对于 D_i 位置对应的随机数
LPR	位置证明生成请求
ELP_i	某一授权位置证明
RC	位置证明验证请求信息

（2）签名设备 D_W：当附近的 D_W 收到位置证明生成请求 LPR 并决定为这个开锁设备生成位置证明的时候，它会通过发回一个应答报文 Ack，此应答报文用于告知 D_i 收到请求并准备为其生成位置证明。

（3）开锁设备 D：开锁设备 D_i 收到 n 个签发设备 D_W 来发的 Ack 后，将自己的私钥 $k_{U_i}^-$ 通过门限秘密共享方式分成 n 份子密钥，子密钥生成方法如下，其度为 k：

$$f(x) = a_0 + a_1 x + \ldots + a_k x^k \tag{2}$$

其中 a_i，$i \in [0, k]$ 为一组非零随机整数，$a_0 = k_{U_i}^-$ 。对于 n 个签名设备 D_W，它们每一个将要接收到的子密钥依次为：

$$\begin{aligned} K_1 &= f(1), \\ K_2 &= f(2), \\ &\ldots \\ K_i &= f(i), \\ &\ldots \\ K_n &= f(n) \end{aligned} \tag{3}$$

生成子密钥集合 $\{K_i \mid i \in \{1,2,\ldots,n-1,n\}\}$ 后，D_i 同时使用 D-H 协议[16-17]对于所有的签发设备 D_W 的协商生成一个临时通信密钥 k_p，并向对应的 D_{Wi} 发送用此密钥加密后的子密钥 K_i 的报文 LPK：

$$LPK = E_{k_p}(K_i) \tag{4}$$

其中 $E()$为高级加密算法 AES，同时为了保证私钥密钥不会被泄露，开锁设备在不同时间地点生成的子密钥不同。

（4）签名设备 D_W：D_{Wi} 接收到 LPK 后，通过临时通信密钥 k_p 解密出子密钥 K_i，然后为 D_i 生成未授权的位置证明 LP：

$$LP = Comm(ID_{Di}, r_{Di}) \big| Comm(L, r^L_{D_{Wi}}) \big| E_{k_p}(K_i) \tag{5}$$

其中 L 是 D_i 发送位置证明生成请求 LPR 时包含的位置信息，$r^L_{D_{Wi}}$为 Commitment 机制中 D_{Wi} 对于 D_i 位置对应的随机数，为减少传输信息量同时提高安全性能，本文采取哈希函数 SHA3-64 来生成此随机数：

$$r^L_{D_{Wi}} = h(L \big| ID_{D_{Wi}}) \tag{6}$$

LP 生成之后，D_{Wi} 将使用自己的私钥 $k^-_{D_{Wi}}$ 为 LP 生成签名，并用智能锁远程管理服务器 SLMS 的公钥 K^+将 LP、与 D_i 临时通信密钥 k_p 以及自身标识加密后，生成授权位置证明 ELP：

$$ELP = E_{K^+}(ID_{D_{Wi}} \big| k_p \big| LP \big| E_{k^-_{D_{Wi}}}(LP)) \tag{7}$$

D_{Wi} 将此授权的位置证明 ELP 和它对于 D_i 的位置 Commit 的随机数 $r^L_{D_{Wi}}$分别发送给 D_i。

（5）开锁设备 D：假定 D_i 成功从 n 个 D_{Wi} 收到了授权的位置证明 ELP，它使用这 n 个 ELP 为自己生成最终的位置证明 FLP：

$$FLP = ELP_1 \big| r^L_{D_{W1}} \big| ELP_2 \big| r^L_{D_{W2}}, \ldots, \big| ELP_n \big| r^L_{D_{Wn}} \big| L \big| t \tag{8}$$

2.3.3 位置证明验证

（6）开锁设备 D：当某一开锁设备 D_i 想要对智能锁远程管理服务器 SLMS 在某一时刻 t 在位置 L 时，首先它按照上一章节步骤生成自己的最终位置证明 FLP，然后它将自己的身份标识 ID_{Di} 与位置证明生成时 LPR 中 Commit 的随机数 r_{Di} 一同发送给 SLMS 进行验证，此验证请求信息记为 RC：

$$RC = ELP_1 \big| r^L_{D_{W1}} \big| ELP_2 \big| r^L_{D_{W2}}, \ldots, \big| ELP_n \big| r^L_{D_{Wn}} \big| L \big| t \big| ID_{Di} \big| r_{Di} \tag{9}$$

（7）智能锁远程管理服务器 SLMS：接收到 D_i 发来的验证请求信息 RC 后，将提取每个位置证明、D_i 的身份标识和它的 Commit 中的随机数并组成一个新信息，此信息记为 Re：

$$Re = ELP_1 \big| ELP_2, \ldots, ELP_n \big| ID_{Di} \big| r_{Di} \tag{10}$$

（8）智能锁远程管理服务器 SLMS：当 SLMS 提取出 Re 后进行两个步骤，第一步对 ELP_i 有效性进行验证，第二步从 Re 中恢复出 D_i 的私钥 k^-_{Ui}来辨别是否用户进行了合谋欺骗攻击。

为了验证 ELP_i 的真实有效性，本文首先使用智能锁远程管理服务器 SLMS 公钥 K^+对 ELP_i 解密，然后通过标识信息 $ID_{D_{Wi}}$ 匹配 D_{Wi} 的私钥。接着判断 $E(LP)$解密后的 LP 与 ELP_i 直接包含的 LP 是否一致，此为验证签发设备 D_{Wi} 授权的时间地点与开锁设备 D_i 请求证明的时间地点是否一致。最后用解析的 $r^L_{D_{Wi}}$、L、ID_{Di}、r_{Di}对 $Comm(L, r^L_{D_{Wi}})$和 $Comm(ID_{Di}, r_{Di})$进行 de-committed 验证。

如果 n 个 ELP 都通过了上述验证步骤那么进行第二步，从 Re 中解密出所有的子密钥 K_i，然后恢复出 D_i 的私钥与 k^-_{Ui} 进行比对。如若没有通过上述验证步骤代表此位置证明不可信。原私钥恢复过程如下：

对于子密钥集合{K_i | i∈{1,2,…,n-1,n}}本文利用门限秘密贡献理论，从中选取任意 k+1 个子密钥，其生成多项式 $f(x)$可以使用拉格朗日插值定理恢复出来：

$$f(x) = \sum_{j}^{k+1} m_j n_j(x) \tag{11}$$

其中，m_j 对应某个子密钥 K_i，x 对应签名设备 D_W 的编号，每个拉格朗日基本多项式 $n_j(x)$表达如下：

$$n_j(x) = \prod_{i=0, i\neq j}^{k+1} \frac{x - x_i}{x_j - x_i} \tag{12}$$

当恢复出 $f(x)$后，令 $x = 0$,即 $f(0) = a_0 = k^-_{Ui}$ ，获得 D_i 原私钥。若恢复出的密钥与原密钥 k^-_{Ui} 保持一致，则表明 D_i 不是与其他恶意攻击者合谋生成的虚假位置证明，SLMS 允许其进行下一步发送开锁指令。反之，则返回位置证明不真实反馈 Ack。

2.4 时间戳加密机制

（10）开锁设备 D：当完成了位置证明之后，开锁设备 D_i 被允许与安全智能锁 SSL_i 发送开锁指令，首先，D_i 通过蓝牙（Bluetooth）与 SSL_i 建立连接，对其发送一个心跳包 OP，用来确认连接建立是否成功：

$$OP = ID_{Di} \big| E_{k^-_{Ui}}(res, t) \tag{13}$$

其中 $E()$为高级加密算法，如 AES，res 为标识信息，告知 SSL_i 此为心跳包，t 为当前时间，ID_{Di} 为开锁设备身份标识，用来记录用户身份。

（11）安全智能锁 SSL：SSL_i 通过使用 SLMS 通过 NB-IoT 网络发来的私钥 k^-_{SSLi}对 OP 进行解密，对于授权用户，其 $k^-_{SSLi} = k^-_{Ui}$，解密成功后，比对自己的时间 t'，如果 | $t-t'$ | >1 小时，代表此信息为重放信息，可能被恶意用户实施了重放攻击，拒绝回复 D_i 。反之则回复一个确认信息 $Comfirm$。

（12）开锁设备 D：当 D_i 收到确认信息 $Comfirm$ 后，代表连接成功建立，并对 SSL_i 发送开锁指令 $Unlock$：

$$Unlock = ID_{Di} \big| E_{k^-_{Ui}}(Open(), t) \tag{14}$$

其中 $Open()$为开锁动作，当 SSL_i 收到 $Unlcok$ 指令后，通过私钥提取出 $Open()$与指令发送时间 t，若 t 与自身时间差在允许范围内，则执行开锁动作，若时间差超过了允许范围，则拒绝此开锁指令。

3　系统实现及性能评估

3.1　实验环境

本文在 MSP430F5438A、Windows ServerR2、华为 P9 等设备上实现了该 NB-IoT 安全智能锁方案，并对本方案各项性能

指标进行了测评。本方案实验测试环境如下：智能锁远程管理服务器 SLMS 配置为 Inter(R) Xeon（R）CPU E5-2682 v4 @2.50GHz 处理器，2GB 主存；安全智能锁 SSL 使用 MSP430F5438A 开发，其性能参数为 16 位超低功耗微控制器，256KB 闪存，16KB RAM，所使用的 NB-IoT 模块为移远 BC95，其上行速率为 62.5kbps，下行速率为 24kbps，所用蓝牙型号为 DialogDA14580；开锁设备 D 使用华为 P9 手机，其配置为 3GB 运行内存，麒麟 955 处理器；采用 128bit 密钥作为 AES/ECB 模式下对称加密密钥，本文主要测试了本方案对于不同种攻击情况下的安全性能、私钥泄露情况以及开锁花费时间。

3.2　安全性对比

为了更加直观反映本方案的安全性能，这一小节通过将本文方案与已有方案[20-22]进行了比较，比较结果如表 2 所示，可以看出，其中对于假冒攻击，即恶意用户截取身份信息与开锁指令，上述四种方案通过加密算法均能较好抵御这一攻击；对于重传攻击，上述第一种方案由于无法提供时间信息，如果用户截取开锁信息加以复制，系统并不能识别出用户是否为授权用户，而文献[20-21]及本文方案开锁过程中会验证时间信息，能够有效抵御此攻击；对于合谋攻击，其中对于位置证明的验证将起关键作用，文献[22]中提到的 Stamp 机制对于检测用户—签名设备合谋存在不足，而本文方案可以有效抵御用户—用户以及用户—签名设备合谋。

表 2　本文方案与文献[20~22]的比较

方案	抵御假冒攻击与否	抵御重传攻击与否	抵御合谋攻击与否
文献[20]	抵御	否	否
文献[21]	抵御	抵御	否
文献[22]	抵御	抵御	部分抵御
本文方案	抵御	抵御	抵御

3.3　系统开销测试

为测试本文方案可行性，本文设计了一个运行与安卓平台的 APP 以及一个 Windows 操作环境下的服务器接口，实现文献[20-22]和本文方案中的基本功能。理想环境中，蓝牙最大传输距离可达 100 米，本文将进行位置证明的设备放置于空旷区域，并设定设备间距离 *dist* 为 10 至 50 米不等。

如图 3、4 所示，文献[20-22]由于没有进行位置证明生成及验证过程，其开锁花费时间和通信开销较少，但存在安全性不足的问题，同时对于公租房情况下，不合法用户转租现象不能很好地遏制。Stamp 方案同本文方案需要进行位置证明，其通信开销较大，但任然处于可以接受的范围。由于 Stamp 机制中设定的距离测试交互协议十分耗时，完成位置证明过程所需要的时间远大于本文方案，其通信开销也稍大于本文方案。

3.4　安全性测试

针对公租房迫切需要解决的转租问题，其关键在于能否验证用户位置证明真实性，本文在不诚实用户相互合谋进行假冒、重放、合谋攻击的情况下，进行了多组实验，验证本文方案能否检测出这些虚假位置证明情况以及是否会泄露诚实用户私密密钥。

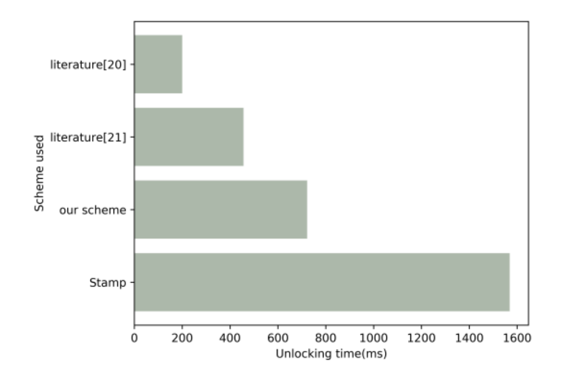


图 3　开锁过程花费时间比较

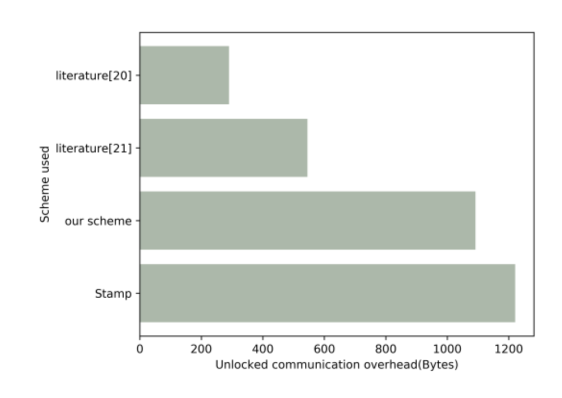


图 4　开锁过程通信开销比较

图 5 反映了本文方案对于用户生成的虚假位置证明的检验情况。理论上本文方案检测率能够达到 100%，从侧面也反映了本文方案的有效性。

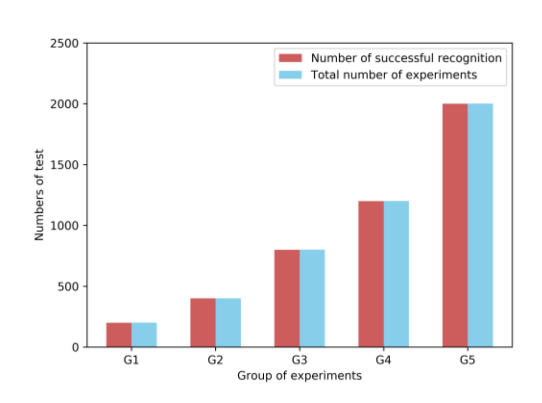


图 5　本文方案对恶意攻击检测效率

图 6 反映了签名设备数量对用户私钥 $k_{U_i}^{-}$ 泄露的影响情况，在签名设备数量大于 2 时，本文方案可以较好地保护用户私钥不被泄露。通过上述实验，本文可以看出，本文方案在拥有低延时和较小通信开销的同时，能够抵御多种攻击，并且高效地检测出恶意用户伪造的虚假位置证明。

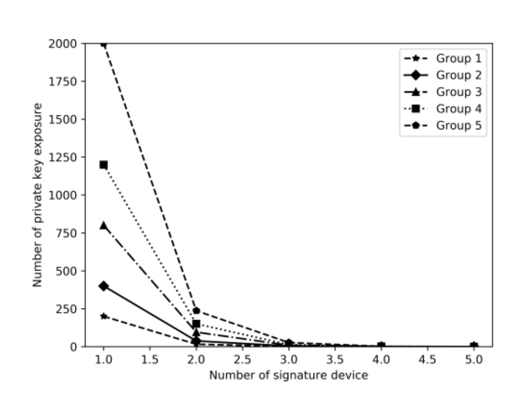


图 6　签名设备数量对私钥泄露的影响

4　结束语

本文致力于解决公租房实施遇到的安全、转租、管理问题，提出了一个基于 NB-IoT 的安全智能锁系统解决方案。它能通过位置证明机制、时间戳机制让用户安全可靠地进行开锁并且能抵御假冒攻击、重放攻击、合谋攻击等多种潜在危险因素，从而能在较低的系统开销情况下，减少用户开锁时间，以获得较佳的用户体验和较高安全性能。通过理论分析及大量仿真实验结果，本文证明了本方案具有较高安全性和较低系统开销。考虑将该方案应用于逐步增长的 NB-IoT 市场下的新型智能家居管理，是本文后期的研究计划。

参考文献：

[1] 孙洁，朱喜钢，宋伟轩，等. 贫困分散还是再集中：收储公租房的效应研究——基于江苏常州的实证 [J]. 城市规划, 2017, 41 (10): 31-38. (Sun Jie, Zhu Xigang, Song Weixuan, *et al.* Poverty deconcentration or reconcentration: an empirical study of the effects of collected public housing in Chanhzhou, Jiangsu Province [J]. Planning Studies, 2017, 41 (10): 31-38.)

[2] 田军. 公租房运行机理与监管方式找寻 [J]. 改革, 2015 (11): 142-150. (Tian Jun. Operating mechanism and supervision of public rental housing [J]. Reform, 2015 (11): 142-150.)

[3] 黄蔚. 北京市公共租赁住房后期管理研究 [D]. 清华大学, 2014. (Huang Wei. Research on post-management of public rental housing in Beijing [D]. Tsinghua University, 2014.)

[4] Hancke G P, Silva B C, Jr H G. The role of advanced sensing in smart cities [J]. Sensors, 2012, 13 (1): 393.

[5] Atzori L, Iera A, Morabito G. From"smart objects"to"social objects": The next evolutionary step of the internet of things [J]. IEEE Communications Magazine, 2014, 52 (1): 97-105.

[6] Wang Y P E, Lin Xingqin, Adhikary A, *et al.* A Primer on 3GPP Narrowband Internet of Things [J]. IEEE Communications Magazine, 2017, 55 (3): 117-123.

[7] Ratasuk R, Vejlgaard B, Mangalvedhe N, *et al.* NB-IoT system for M2M communication [C]// Proc of Wireless Communications and NETWORKING Conference. IEEE, 2016: 428-432.

[8] Tang Wan, Chen Min, Ni Jin, *et al.* Security Enhancement Mechanism Based on Contextual Authentication and Role Analysis for 2G-RFID Systems [J]. Sensors, 2011, 11 (7): 6743-59.

[9] 高福友. 低功耗指纹锁无钥匙门禁系统设计及协议制定 [J]. 计算机工程与设计, 2011, 32 (03): 887-891. (Gao Fuyou. Design and establishment of low power consumption fingerprint lock remote keyless entry system and communication protocol [J]. Computer Engineering and Design, 2011, 32 (03): 887-891.)

[10] 薛琳，魏兰磊，朱述川，等. 基于 GPRS 和 RFID 技术的门禁控制系统 [J]. 电子技术应用, 2012, 38 (06): 145-148. (Xue Lin, Wei Lanlei, Zhu Shuchuan, *et al.* Design of door access control system based on GPRS and RFID [J]. Computer Technology and Its Applications, 2012, 38 (06): 145-148.)

[11] 应时彦，周泽育，梅一珉. 一种基于 ZigBee 的联网型无线门锁系统设计 [J]. 浙江工业大学学报, 2017, 45 (02): 153-158. (Ying Shiyan, Zhou Zeyu, Mei Yimin. A design of networked wireless lock system based on ZigBee [J]. Journal of Zhejiang University of Technology, 2017, 45 (02): 153-158.)

[12] Feng Yuxiang, Wang Wenhao, Weng Yukai, *et al.* A Replay-Attack Resistant Authentication Scheme for the Internet of Things [C]// Proc of IEEE International Conference on Computational Science and Engineering. IEEE, 2017: 541-547.

[13] Callegati F, Cerroni W, Ramilli M. Man-in-the-Middle Attack to the HTTPS Protocol [J]. IEEE Security & Privacy, 2009, 7 (1): 78-81.

[14] Liu Mengjun, Liu Shubo, Zhang Rui, *et al.* Privacy-preserving distributed location proof generating system [J]. 中国通信（英文版）, 2016, 13 (3): 203-218.

[15] Lu Chihchung, Tseng Shauyin. Integrated design of AES (Advanced Encryption Standard) encrypter and decrypter [C]// Proc of IEEE International Conference on Application-Specific Systems, Architectures, and Processors. IEEE Computer Society, 2002: 277.

[16] Shamir A. How to share a secret [M]. ACM, 1979.

[17] Naor M. Bit commitment using pseudorandomness [J]. Journal of Cryptology, 1991, 4 (2): 151-158.

[18] Liu Weiran, Liu Jianwei, Wu Qianhong, *et al.* SAKE: scalable authenticated key exchange for mobile e - health networks [J]. Security & Communication Networks, 2016, 9 (15): 2754-2765.

[19] Diffie W, Hellman M E. New directions in cryptography [J]. IEEE Transactions on Information Theory, 1976, 22 (6): 644-654.

[20] 黄鹤松，刘容良，郭恒兰，等. 一种基于 CPU 卡的门禁系统的设计 [J]. 电子技术应用, 2017, 43 (01): 137-140+144. (Huang Hesong, Liu Rongliang, Guo Henglan, *et al.* The design of access control system on CPU card [J]. Computer Technology and Its Applications, 2017, 43 (01): 137-

140+144.)

[21] 胡向东，唐飞. 智能家居门禁系统的安全控制方法 [J]. 重庆邮电大学学报：自然科学版，2016, 28 (06): 863-869. (Hu Xiangdong, Tang Fei. Secure control methods of the entrance guard system for smart home [J]. Journal of Chongqing University of Posts and Telecommunication: Natural Science Edition, 2016, 28 (06): 863-869.)

[22] Wang Xinlei, Zhu Jindan, Pande A, *et al.* STAMP: Ad hoc spatial-temporal provenance assurance for mobile users [C]// Proc of IEEE International Conference on Network Protocols. IEEE, 2013: 1-10.